Petit théorème de Fermat

Maths Expertes · Terminale · Bac

Énoncé · 2 formes

Soit p un nombre **premier** et $a \in \mathbb{Z}$.

Forme 1 · si $p \nmid a$:

$$a^{p-1} \equiv 1 \pmod{p}$$

Forme 2 · pour **tout** a :

$$a^{p} \equiv a \pmod{p}$$

→ F1 → F2 : multiplier par a.

→ Si $p \mid a$: $a \equiv 0$ donc $a^p \equiv 0 \equiv a$.

Contexte & cadre

Fermat · 1640
Énoncé sans preuve, communiqué dans une lettre

Euler · 1736
Démontre le théorème + généralise à $\varphi(n)$

→ À ne pas confondre avec le **grand théorème de Fermat** ($x^n + y^n = z^n$, Wiles 1995)

→ Outil **central** de l'arithmétique modulaire et de la **cryptographie** (RSA)

Attention · p doit **impérativement** être premier. Faux si p composé (cf. pseudo-premiers).

Idée de démonstration

Pour p premier, $p \nmid a$: les $p-1$ **classes** :
$\{a,\ 2a,\ 3a,\ \ldots,\ (p-1)a\} \pmod{p}$
sont une **permutation** de $\{1, 2, \ldots, p-1\}$.

En multipliant : $a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$$

Or $(p-1)! \wedge p = 1$, on simplifie : $a^{p-1} \equiv 1 \pmod{p}$ ✓

Méthode · calculer $a^n \pmod{p}$

Recette en **2 étapes** :

1. Division eucl. de n par $p-1$: $n = (p-1)q + r$.
2. $a^n = (a^{p-1})^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{p}$.

Ex · reste de $3^{100} \pmod 7$: $p = 7$, $3^6 \equiv 1$.
$100 = 6 \times 16 + 4$ donc $3^{100} \equiv 3^4 = 81 \equiv 4 \pmod 7$.
→ Reste $= 4$

Exemple détaillé · $2^{100} \pmod{13}$

$p = 13$ premier, $13 \nmid 2$. **Fermat** : $2^{12} \equiv 1 \pmod{13}$.

Division : $100 = 12 \times 8 + 4$
$2^{100} = (2^{12})^8 \cdot 2^4 \equiv 1^8 \cdot 16 \pmod{13}$
$16 = 13 + 3 \equiv 3$
→ $2^{100} \equiv 3 \pmod{13}$

Sans Fermat : il aurait fallu calculer la périodicité à la main (longue).

Inverse modulo un premier

Si p premier et $p \nmid a$:

$$a \cdot a^{p-2} \equiv 1 \pmod{p} \quad \rightarrow \quad a^{-1} \equiv a^{p-2} \pmod{p}$$

Découle de $a^{p-1} \equiv 1$, en isolant a^{p-2}.

Ex · inverse de $3 \pmod 7$: $3^{7-2} = 3^5 = 243$.
$243 = 34 \times 7 + 5$ → $3^{-1} \equiv 5 \pmod 7$
Vérif : $3 \times 5 = 15 \equiv 1 \pmod 7$ ✓

Test de primalité · pièges

Si n premier : $\forall a$ premier avec n, $a^{n-1} \equiv 1 \pmod{n}$.

Test pratique : choisir a et calculer $a^{n-1} \pmod{n}$. Si $\neq 1$: n est **composé**.

La réciproque est FAUSSE.
→ **Pseudo-premiers** de Fermat en base a : composés qui passent le test.
→ **Nombres de Carmichael** : composés qui passent le test pour toutes les bases (ex : $561 = 3 \cdot 11 \cdot 17$).

→ Tests modernes (Miller-Rabin, AKS) reposent sur des renforcements de Fermat.

Application · RSA

Soit $n = pq$ avec p, q premiers, $\varphi(n) = (p-1)(q-1)$.

Fermat appliqué à p et q donne :

$$m^{ed} \equiv m \pmod{n} \quad \text{quand} \quad ed \equiv 1 \pmod{\varphi(n)}$$

→ **Chiffrement** : $c = m^e \pmod n$
→ **Déchiffrement** : $m = c^d \pmod n$
→ Sécurité = difficulté de **factoriser** n

Récap · à connaître par cœur

Cas	Hypothèse	Résultat
Forme 1 PTF	p premier, $p \nmid a$	$a^{p-1} \equiv 1 \pmod p$
Forme 2 PTF	p premier, $a \in \mathbb{Z}$	$a^p \equiv a \pmod p$
Inverse	p premier, $p \nmid a$	$a^{-1} \equiv a^{p-2} \pmod p$
Calcul $a^n \pmod p$	$n = (p-1)q + r$	$a^n \equiv a^r \pmod p$
Euler (généralisation)	$a \wedge n = 1$	$a^{\varphi(n)} \equiv 1 \pmod n$

Cycles modulo petits premiers

p	$p-1$	Ordre max
3	2	$a^2 \equiv 1$
5	4	$a^4 \equiv 1$
7	6	$a^6 \equiv 1$
11	10	$a^{10} \equiv 1$
13	12	$a^{12} \equiv 1$

L'**ordre** de a divise toujours $p-1$ (Lagrange).

Ex · $2^6 \equiv 1 \pmod 7$: ordre de 2 divise 6.
$2, 4, 1$: ordre 3 (divise bien 6 ✓).